PATENT

In The United States Patent And Trademark Office

Appl. No.:	09/518,583	Confirmation No.: 5843
Applicant(s):	Chee-Seng Chow, et al.	
Filed:	March 3, 2000	
Art Unit:	2134	
Examiner:	Ellen C. Tran	
Title:	SYSTEM AND METHOD FOR ACCESSING A REMOTE SERVER FROM AN INTRANET WITH A SINGLE SIGN-ON	

Docket No.:	047138/257085	February 23, 2007
Customer No.:	00826	

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF UNDER 37 C.F.R. § 41.41

This Reply Brief is submitted in response to the Examiner's Answer mailed December 29, 2006. In light of the Examiner's Answer, Applicants submit rebuttal arguments to address the rejections under 35 U.S.C. §§ 102(e) and 103(a), as well as clarify arguments previously submitted in the Substitute Appeal Brief.

Applicants submit that none of the cited references teach or suggest sending a token to a remote server that contains authentication information responsive to a first authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user, as recited by independent Claims 1, 11, 21, and 22. The Examiner relies on various portions of Win for disclosing this particular recitation of the claimed invention. Namely, in the Response to Arguments the Examiner relies on the ability to modify profiles and roles using the Authentication Client Module (col. 9, lines 33-45; col. 11, lines 21-26), and on the capability of the Administration Application to create, delete, and modify user resource and role records (col. 13, lines 2-52; col. 19, lines 6-34). Moreover, the Examiner finds that because Win discloses retrieving profile information that includes IP

address, user's name, and a user's role, that such information is added to the cookie and would be capable of being modified or changed using the Administration Application (col. 10, lines 43-55; col. 19, lines 6-34).

Applicants respectfully disagree with the Examiner's assertions and reiterate that Win does not teach or suggest sending a token to a remote server that contains authentication information responsive to a first authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user, as recited by the claimed invention. As disclosed in the Substitute Appeal Brief, the present application discloses that the token may include various fields, including authentication information and a field for a new user flag that is sent when the Intranet server detects a new user. (FIG. 8; Page 16, lines 12-15). The embodiment depicted by FIG. 9 of the present application adds the capability to transmit updated user profile information to the remote server. In this vein, independent Claims 1, 11, 21, and 22 recite that the token contains authentication information regarding a new account and an update to an existing account for the user. Applicants submit that Win only discloses creating a user cookie and roles cookie that contain a subset of the user's profile information and roles, respectively. Col. 10, lines 51-55. The user and roles cookies are encrypted and returned to the user's browser and sent to each Web server that the user accesses. Col. 10, line 67 – Col. 11, line 2. Only those cookies that are unexpired are saved on a mass storage device at the user's browser, such as a disk drive at the user's client machine or terminal. Col. 11, lines 2-6. Furthermore, Win does not disclose the ability to modify user information contained on the cookie but, rather, discloses that the Authentication Client is capable of modifying a user's account information and roles that are stored at the Registry Repository. In particular, Win discloses:

> Registry Repository 110 is the primary data store for the system 2. It contains data on Users, Resources and Roles and configuration information required for the system 2 to function. Selected data, for example, passwords, are stored in Registry Repository 110 in encrypted form. The data about Users, Resources and Roles stored in Registry Repository 110 represents the structure of an enterprise or organization that has protected resources. Data in Registry Repository 110 is managed using Administration Application 114. Col. 12, lines 32-40.

Moreover, Win discloses that the "Administration Application 114 can create, delete, modify and records in the Registry Repository 110; assign roles; perform bulk operations; generate reports; and configure the system," wherein "the user record profile information includes the user's first and last names, email address, login name, password, locale, whether the account is active or inactive, and when the password or account will expire." Col. 13, lines 2-16.

Therefore, contrary to the Examiner's assertions that the cookies of Win include information that may be modified, separate data files are stored at the Registry Repository and are capable of being modified. In fact, the Authentication Client of Win creates the cookies by requesting profile information at the Registry Server in order to create the user cookie and role cookie, each cookie including a subset of user profile or roles information. Col. 10, lines 45-55.

In any event, despite generally disclosing that user profile or roles information may be updated or modified, Win does not disclose that the cookies contain authentication information regarding a new account and/or an update to an existing account for the user, as the cookies are created by the Authentication Client based on stored information within the Registry Server. Thus, the cookies are only subsets of user information stored remotely at the Registry Server, and Win does not teach or suggest that any new or updated user information is provided on the cookies. Simply providing the capability to update or add a new account is significantly different than providing information regarding a new account or an update to an existing account with a token to a remote server, as recited by the claimed invention.

Furthermore, independent Claims 1, 11, 21, and 22 recite selecting a remote server subsequent to the first authentication and sending a token to said remote server. In contrast, Win discloses that updating the profile information may be achieved when a user's profile or locale information is updated via the Authentication Client, which is associated with the Access Server (see FIG. 4 of Win), not the Protected Server that contains protected resources that the user is attempting to access and that receives cookies sent for authentication (see FIGS. 2 and 3A-3C of Win). Thus, user and roles cookies are sent to the Protected Server, where the cookies were previously created in response to a login request at the Access Server and which contains only a subset of information stored at the Registry Server. As such, the cookies sent to the Protected Server do not contain authentication information regarding a new account and/or an updated account for a user, which is unlike the claimed invention.

As such, it is apparent that none of the cited references, taken alone or in combination, teach or suggest sending a token to a remote server that contains authentication information responsive to a first authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user, as recited by independent Claims 1, 11, 21, and 22. For the forgoing reasons as well as for the additional reasons set forth in the Substitute Appeal Brief, Applicants submit that the rejection of Claims 1-22 under 35 U.S.C. §§ 102(e) and 103(a) are overcome.

Respectfully submitted,

Trent A. Kirk
Registration No. 54,223

CUSTOMER NO. 00826
ALSTON & BIRD LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
Tel Charlotte Office (704) 444-1000
Fax Charlotte Office (704) 444-1111

ELECTRONICALLY FILED USING THE EFS-WEB ELECTRONIC FILING SYSTEM OF THE UNITED STATES PATENT & TRADEMARK OFFICE ON February 23, 2007.